**Montana State Information Security Advisory Council (MT-ISAC)**
**Minutes**
**June 21, 2017**
**1:00 PM**
**Cogswell Building, Room 151**

**Members Present:**

Ron Baldwin, State CIO/SITSD – Chair
Lynne Pizzini, SITSD – Vice Chair
Jesse Callendar, MATIC/DOJ
Joe Chapman, DOJ
Kreh Germaine, DNRC
Adrian Irish, UM
Margaret Kauska, DOR
Manuel Soto, OPI
Madison Iler, LMG Security – Alternate
Carroll Benjamin, DMA – Alternate
Erika Billiet, City of Kalispell
Stuart Fuller, DPHHS

**Staff Present:** Joe Frohlich, Wendy Jackson, Sarah Mitchell

**Guests Present:** Tom Murphy, Dave Johnson, Mike Bousliman, Marieke Baughman, Lance Wetzel, Rebecca Cooper, Tim Kosena, Craig Marquardt, Sean Rivera, Jerry Marks

**Real-time Communication**: Dana Corson, Zach Day, Phillip English, Alan Grover, Brian Jacobson, Michael Jares, Suzi Kruger, Darrin McLean, Terry Meagher, Cheryl Pesta, Jessica Plunket, Rawlin Richardson, Edward Sivils, Erin Stroop, David Swenson, Paul Kozlowitz, Billie Byrd, Josh Rutledge, Michael Barbere, Jerry Kozak, Larry Krause, Erin Dunkin, Christie Mock, Judy Kelly, Angie Riley, Irv Vavruska, Joshua Tuman, Anne Kane, Mike Mazanec

**Welcome**

Ron Baldwin welcomed the council to the June 21, 2017 MT-ISAC meeting. All members and guests were introduced.

**Minutes**

**Motion:** Margaret Kauska made a motion to approve the May 10, 2017 minutes. Jesse Callendar seconded the motion. Motion carried.

**Business**

**Data Loss Prevention (DLP)**

Joe Frohlich provided an update regarding DLP. MT-ISAC council members completed a survey to determine agency preparedness regarding the July 1, 2017 DLP go live date. Based on the survey results, the go live date for DLP on Exchange has been revised to October 1, 2017. Agencies wishing to roll out DLP prior to October may open a case with the Service Desk to create a mail enabled Active Directory (AD) Security group; this may be done by individual bureaus or the entire agency. Users cannot be nested within another group. Anticipated go live dates must be included in the ticket. MT-ISAC has provided agencies with a notice to communicate DLP information to users.

**Email Security**

Mr. Frohlich stated the Department of Administration (DOA) policy dictates blocking of all password protected files. DOA policy also prohibits whitelisting of emails. Dave Johnson reviewed the Microsoft Enterprise Agreement (EA) with Advanced Threat Protection (ATP) recently purchased for licensed AD users. ATP scans all external attachments, emails, and hyperlinks for malicious activity. Hyperlinks are verified by monitoring and comparing hyperlink behavior against identified malware. Users will receive notification regarding attachments and hyperlinks deemed unsafe. Microsoft EA does not guarantee blocking of phishing attempts within the Uniform Resource Locator's (URL). ATP will delay incoming email delivery an average of two to three minutes. On occasion, emails with attachments or hyperlinks may require up to 30 minutes for processing. Internal pilots will begin in July 2017. Additional information will be provided in future MT-ISAC and Network Managers Group (NMG) meetings.

**SentinelOne**
Mr. Frohlich noted the State Information Technology Services Division's (SITSD) SPLUNK team is working with SentinelOne to build a dashboard for each agency. SITSD has established connection with the SentinelOne console and performed limited testing with Application Programming Interfaces (APIs). Agencies interested in participating in SentinelOne testing can submit a case to Service Desk. Agencies will then receive a link with agents to install on servers. Following successful Proof of Concept (POC) testing, SITSD plans to purchase SentinelOne for each server and install it on all SITSD workstations. Agencies will be responsible for deployment and installation on their servers. With this tool, agencies will be able to monitor servers, receive alerts, and perform actions and exemptions through SPLUNK. SentinelOne will become a catalog item for agencies and the university system to purchase with an individual license cost of $62.50 per user. The SentinelOne console will be monitored by SITSD's Network Operation and Security Center (NOSC) and agency's Information Technology (IT) teams. Standards will be established regarding monitoring.

**Action Item:** Mr. Frohlich will schedule a SentinelOne demo.

**Workgroup Updates**
**Best Practices / Tools Workgroup Update**
Lynne Pizzini stated the workgroup is currently exploring development of best practices for media protection, personnel security, vulnerability scanning, and risk management. The workgroup meets on the first Wednesday of each month from 1:00 PM to 3:00 PM.
Individuals interested in participating in the Best Practices Workgroup should contact Joe Frohlich at JFrohlich@mt.gov.

**Situational Awareness / Outreach / Public Safety Workgroup Update**
Mr. Frohlich gave a brief update on workgroup activities. The workgroup observed contacting state associations via phone and follow-up emails regarding the outreach letter was more effective than mailing the letters alone. The workgroup discussed contacting associations to seek feedback regarding the outreach letter.

**Biennium and Review of MT-ISAC**
Mr. Frohlich reviewed the history of MT-ISAC. This information is on the MT-ISAC website located at https://sitsd.mt.gov/Governance/Boards-Councils/MT-ISAC. MT-ISAC's first official meeting was held in August 2015. The council's mission, goals, and objectives were approved in September 2015. Since inception, the council has approved the Information Security Policy and Data Classification Policy, rescinded 28 enterprise security policies, and established in policy several enterprise standards, forms, and guidelines. In addition, 10 workgroups were created to address the 37 objectives for the council. These workgroups were used to establish Best Practices and Situational Awareness groups.
Mr. Baldwin complemented the proactive nature and effective functioning of the MT-ISAC.
Ms. Kauska commented the Best Practices workgroup is a valuable resource for agencies to streamline processing and increase security.
Ms. Pizzini voiced gratitude to agencies for their support and participation in the Best Practices workgroup.
Mr. Frohlich offered thanks to all council members and staff who worked to make the MT-ISAC successful.

**Meet the Threat**
Ms. Pizzini gave a summary of the establishment of the Montana Information Security Advisory Council (MT-ISAC). Based on cyber security advisements received from the National Governor's Association (NGA), recommendations received from groups attending a NGA host event and the ITMC task force, the Governor provided the executive order to form MT-ISAC. The Governor continues to support enforcement and awareness for cyber security through the state's Enterprise Security Program (ESP) and MT-ISAC. Ms. Pizzini provided recommendations to the Governor concerning next steps for the council. These recommendations encompass broadening the focus of the council to include more external representation and appointing General Matthew Quinn as council Chair. Council membership will incorporate representatives from different areas of critical infrastructure and emergency management including government, education, healthcare, banking, technology, and energy providers. The focus of the council will include an emphasis on education. A central institution within Montana will be identified as a Center of Excellence for cyber security education. The council will increase its focus on legislation to include updating statutes and legislation that align with current

cybersecurity needs. MT-ISAC will deliver the message of cyber security in a positive and informational manner to include internal and external outreach programs for critical infrastructure. The council will continue to collaborate with private industry regarding cybersecurity issues. MT-ISAC will aid in the development and expansion of Montana National Guard (MNG) cybersecurity to include penetration testing. The council will work with the Montana Department of Justice (DOJ) to increase cybersecurity education for law enforcement. MT-ISAC will work to increase state and private sector preparedness and response. The council will coordinate with agencies such as the Federal Bureau of Investigation (FBI), Department of Homeland Security (DHS), and the National Guard (NG) in criminal investigative response in cybersecurity incidents. MT-ISAC will explore additional resources for DOJ regarding cyber investigations. The Governor has reviewed and agreed upon these recommendations. A list of recommendations regarding the makeup of MT-ISAC membership for FY18 will be developed. Ms. Pizzini requested suggestions from council members regarding private sector representatives from the banking and healthcare fields. Recommendations should be submitted to Mr. Frohlich at jfrohlich@mt.gov. MT-ISAC goals and objectives will be revised by the next council to align with these recommendations. The Best Practices Workgroup will be maintained as a focus for state agencies to continue participation and input in this council.

**Current Threats**
Sean Rivera provided an update regarding current threats. SITSD continues to perform scans for agencies, ensure agency's implementation of updates, and research vulnerabilities resulting from the WannaCry ransomware campaign. 465,000 devices or systems were impacted or infected by this ransomware campaign. The Multi-State Information Sharing and Analysis Center (MS-ISAC) observed 141 events pertaining to WannaCry, EternalBlue, or DoublePulsar vulnerabilities; however, no infection was detected. A report released by Risk Based Security (RBS) indicated that, in the first quarter of 2017, 1,200 breaches and 3.4 billion records were exposed. Business email compromises, which assume the identity of an individual and request funds transfer or personnel information. The FBI identified 200 organizations in 2017 that have been victims to this scam. Deep Root Analytics on Amazon Web Services (AWS) was publicly accessible from June 1, 2017 to June 12, 2017. The data leak enabled information on 198 million US citizens to be viewed and downloaded. The estimated 1.3 terabytes (TB) of data exposed included individuals' home addresses, birthdates, phone numbers, and political views. In addition, 60,000 documents of sensitive US data exposed through AWS host. Mr. Rivera recommended reviewing all permission settings in the Cloud.

**Open Forum**
**Future Agenda Items**
Joe Chapman requested the council address the issue of agency scans performed by SITSD.
Ms. Pizzini stated the Best Practices workgroup is working on a vulnerability scan best practice to determine frequency of scans. DOJ has asked to perform their own scan in lieu of SITSD scans. Statute dictates DOA holds responsibility for the network, and SITSD is the only department authorized to conduct these scans. If other entities perform network scanning, there is potential that they could scan devices outside of their agencies, which is prohibited. SITSD employees are specifically authorized by the Internal Revenue Service to perform these scans. SITSD is looking to purchase a Governance Compliance System which will integrate scanning and provide agencies with a dashboard to monitor scans. A team of agency representatives will be established to identify a product.

**Action Item**: Mr. Frohlich will reschedule the July 2017 Best Practices Workgroup meeting.
**Action Item:** Mr. Frohlich will ensure this topic is the first item on the agenda for the next meeting of the Best Practices Workgroup.

**Public Comment**
None

**Next Meeting**
July 12, 2017
1:00 PM to 3:00 PM
Capital Building, Room 152

**Adjournment**
The meeting adjourned at 2:34 PM.